Development of a High-Speed Quantum Random Number Generator Harvesting Quantum Phase Fluctuations

ANURAG K S V* | KANAKA RAJU P# | RAGHAVAN G†

*Master's Student, #Assistant Professor, †Professor & Director at School of Quantum Technology, Defence Institute of Advanced Technology, Pune-411025, MH, India

INTRODUCTION

Why Quantum Random Number Generators?

Type of RNG	PRNG	TRNG	QRNG
Source of Randomness	Deterministic	Lack of Knowledge	Inherent

Applications of QRNGs

Quantum Key Distribution | Cryptography & Networking | Simulation & Modelling | Statistics Gaming & Gambling

What is Randomness?

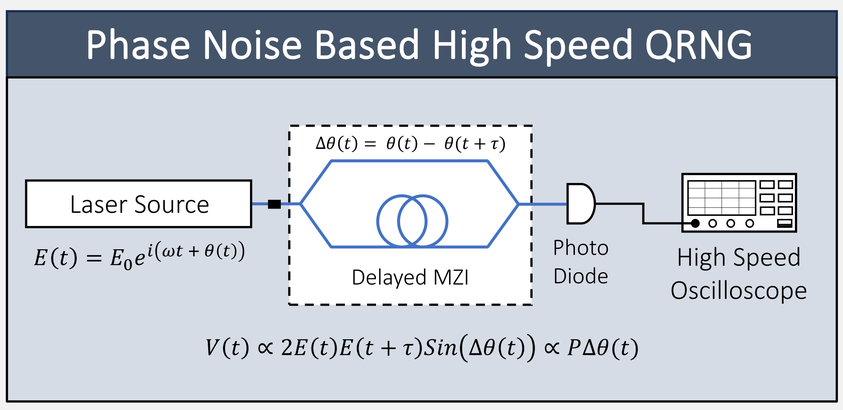
Uniformity (every outcome is equally likely & independent) | Unpredictability (absence of any pattern)

OBJECTIVES

- Development of a **high-speed, low-cost, and reliable quantum random number generator** suitable for quantum key distribution systems and cryptographic applications.
- Perform **high-speed post-processing** on the raw data acquired from the QRNG hardware to obtain **information-theoretically provable** random numbers.
- Perform **standardized randomness tests such as NIST SP 800-22** to verify for **uniformity and unpredictability** in the random numbers output obtained after the post processing to ensure randomness.

PHASE NOISE BASED QRNG

Phase Noise Based High Speed QRNG



Quantum Vacuum Fluctuations → Harvesting Spontaneous Emission → Random Phase Correlation → Phase Noise Measurement

- The inherent **source of randomness** for the Phase Noise based QRNG originates from **Spontaneous Emission**.
- The spontaneous emission phenomenon is inherently random in nature, guaranteed by the quantum randomness associated with **vacuum fluctuations**.
- We implement this physical system through a **self-heterodyne measurement** of the laser's emission, operating it close to the laser's threshold.

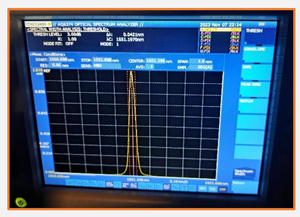
Type	Rate (Order)
Single Photon Splitting	Mbps
Time of Arrival	Mbps
Vacuum Fluctuations	Gbps
Phase Noise	Gbps

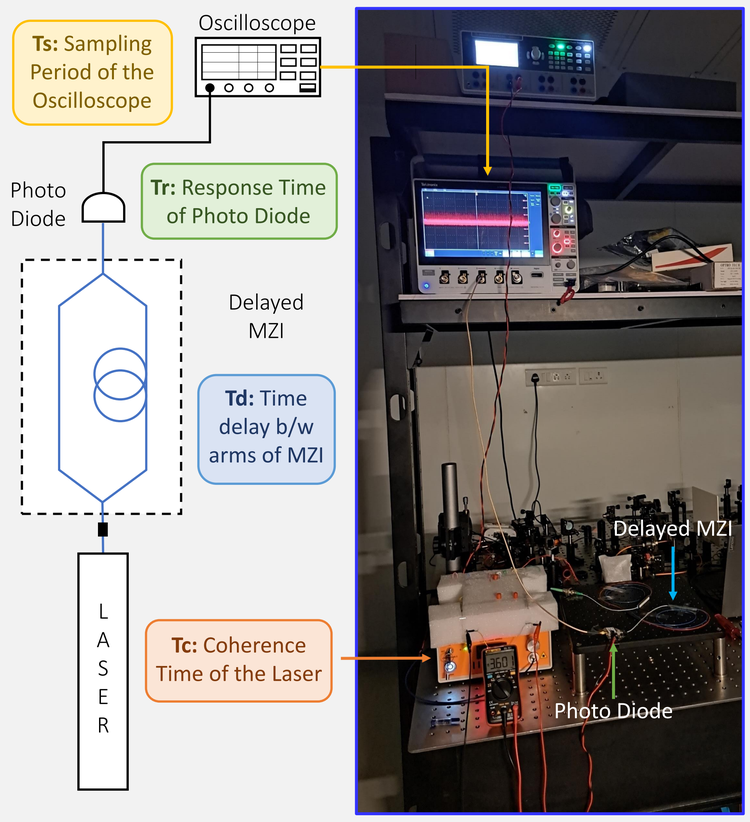
Xu F et. al., Optics Express, 20(11):12366 (2012)

Kollmitzer C et. al., Springer, 9783319725949 (2020)

EXPERIMENTAL DETAILS

- Oscilloscope:
  - (a) Sampling Rate: 250 MS/sec
  - (b) ADC: 8-bit
- Photo Diode:
  - (a) Type: InGaAs
  - (b) Bandwidth: 2.5 GHz
- Fiber Based MZI:
  - (a) Unbalance Length: ~ 50 cm
- Laser:
  - (a) Wavelength: 1551.1970 nm
  - (b) Linewidth: 0.0421 nm / 5.278 GHz

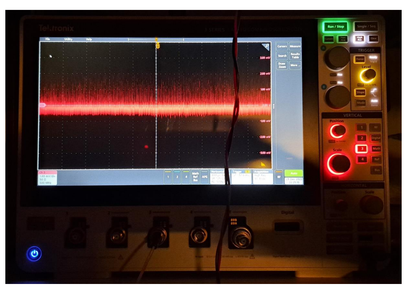


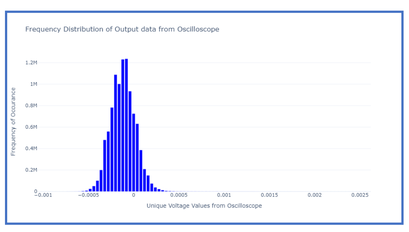


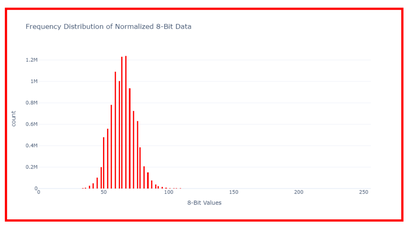
Qi B et. al., Optics Letters, 35(3):312 (2010)

RESULTS

Raw Data Acquisition







QRNG Rate = 250 MS/sec * 8 bits = **2 Gbps**

Algorithmic Schematic for QRNG Post-Processing

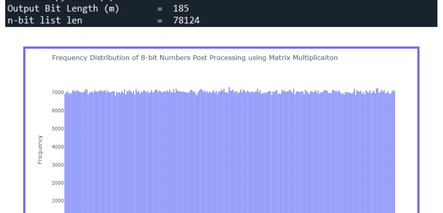
Parameter Estimation → Data Preparation → Randomness Extraction → Random Number Readout

Matrix Multiplication based Toeplitz Hashing

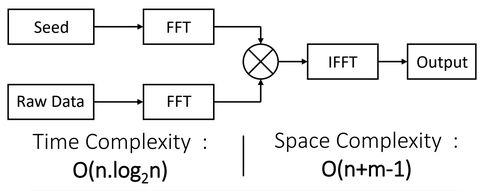
$$\begin{pmatrix} s_m & s_{m+1} & \dots & s_{m+n-2} & s_{m+n-1} \\ s_{m-1} & s_m & \dots & s_{m+n-3} & s_{m+n-2} \\ \vdots & s_{m+1} & \ddots & \vdots & \vdots \\ s_2 & \vdots & \ddots & s_n & s_{n+1} \\ s_1 & s_2 & \dots & s_{n-1} & s_n \end{pmatrix} \times \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_{n-1} \\ d_n \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{m-1} \\ r_m \end{pmatrix}$$

Time Complexity : $O(n^2)$ | Space Complexity : $O(n*m)$

```
In [2]: runfile('C:/Users/anura/Desktop/4) Autumn 2023/QRNG/3rd Semester Review/
code/cpu_matmul.py', wdir='C:/Users/anura/Desktop/4) Autumn 2023/QRNG/3rd
Semester Review/code')
Length of Input Bit-Str (l) =  8
Size of Raw Data Set (s)    =  10000000
Block Size Considered (n)   =  1024
Security Parameter (e)      =  7.888609052210118e-31
Min-Entropy of Raw Data     =  3.02
Min-Entropy at n (k)        =  385
Output Bit Length (m)       =  185
n-bit list len              =  78124
```

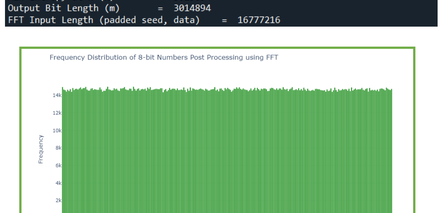


Fast Fourier Transform based Toeplitz Hashing



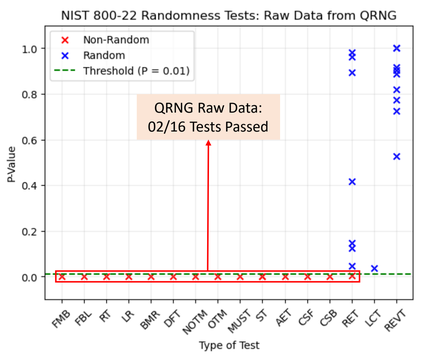
Time Complexity : $O(n.\log_2 n)$ | Space Complexity : $O(n+m-1)$

```
In [1]: runfile('C:/Users/anura/Desktop/4) Autumn 2023/QRNG/3rd Semester Review/
code/gpu_fft.py', wdir='C:/Users/anura/Desktop/4) Autumn 2023/QRNG/3rd Semester
Review/code')
Length of Input Bit-Str (l) =  8
Size of Raw Data Set (s)    =  10000000
Block Size Considered (n)   =  8000000
Security Parameter (e)      =  7.888609052210118e-31
Min-Entropy of Raw Data     =  3.02
Min-Entropy at n (k)        =  3015094
Output Bit Length (m)       =  3014894
FFT Input Length (padded seed, data)    =  16777216
```

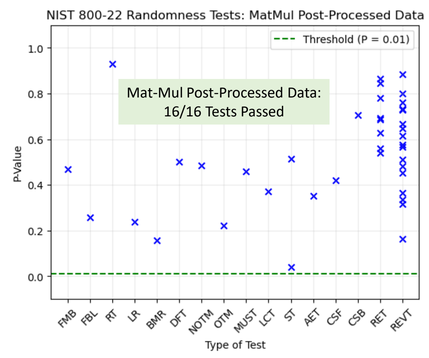


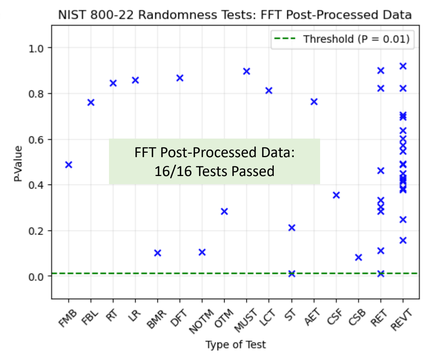
Randomness Tests

NIST SP 800-22	= 16 Tests
DieHard	= 17 Tests
DieHarder	= 31 Tests
TESTU01 (Small Crush)	= 10 Tests



- To verify the randomness of the output generated from the QRNG, we perform the **NIST SP 800-22 Randomness Tests**, which consist of 16 comprehensive tests. These tests check for the uniformity and unpredictability of the output data.
- When the raw data is passed through the test suite, it **passes 2 out of 16 tests** verifying the biased output from the QRNG. However, the post-processed data, which is based on Matrix Multiplication and FFT-based Toeplitz Hashing, **passes all 16 out of 16 tests**.





Ang SK. GitHub. (2022)

Rukhin AL et. al., National Institute of Standards and Technology (US), SP 800-22 (2000)

CONCLUSION

- We achieved a **Raw Data Generation Rate of 2.0 Gbps** with the aforementioned QRNG system, rendering it well-suited for various practical applications in Quantum Key Distribution systems.
- We performed **High-Speed Post-Processing** on the raw data acquired from the Phase Noise based QRNG to obtain **Information-Theoretically Provable** random numbers.
- The post-processed random numbers generated **successfully pass all the NIST SP 800-22 Randomness Test Suite**, ensuring the unpredictability and reliability of the data.

email: anurag.krovvidi@gmail.com
raju@diat.ac.in

website: https://sqt.diat